4.7 Search Systems

Definition of Prohibited Items

A prohibited item (or contraband) is any unauthorized item in a facility. For the purposes of security, a prohibited item is any item or material that can be used to commit an act of theft or sabotage. Potential prohibited items include weapons, tools, explosives, and nuclear material. Other items like drugs, food, and communications equipment (cell phones and radios) may also be prohibited. – use TECDOC 176 definition. Types of searches include hand-, package-, metal detection, explosives, and nuclear material-searches.

Purpose of Prohibited Item Detection System

The objectives of a contraband detection system for use in a physical protection system at a nuclear facility are:

1. to detect and prevent the entry of contraband material (weapons, explosives, and unauthorized tools)

2. to detect and prevent the unauthorized removal of nuclear materials.

Alarm Alerts Guards Who Investigate Cause

An alarm should occur when contraband is detected. Upon receipt of an alarm, guards assess the problem, determine whether the alarm is a nuisance alarm or a valid alarm, and, if necessary, initiate a preplanned response.

All Materials Should be Subject to Search

Where entry is controlled, it is expected that all personnel and material will be examined for contraband. Maintenance tools, food, instruments, building materials, and operating supplies should be examined. When leaving, all personnel and materials (such as operating and construction waste, materials for reclamation, equipment to be repaired, and sewage) should be examined for nuclear materials. Since vehicles are generally difficult to search, most facilities limit the number of vehicles that can enter the facility and require most vehicles to remain inside the controlled area.

Search for Prohibited Items at Protected Areas and Vital Areas

Prohibited item detection systems are considered for use in two specific types of areas: (1) protected areas and (2) inner or vital areas. These areas are shown in section 4.6. More stringent searches may be performed at higher security areas.

Prohibited Item Detection Methods

Prohibited item detection can be done with technology, such as metal, x-ray, canine, explosives detectors, nuclear material detection, or by manual package searches by guards.

Manual or Hand-Search

Manual or hand-searches by guards can be very effective. Training and procedures are very important to achieve high effectiveness with hand-searches. An important consideration is educating the guards on what the threats look like: size, mass, shapes, etc. Manual search is a common secondary screening technique, used to resolve alarms from the technologies described below. Hand searches of people are often referred to as pat-down searches. In principle, and item can be searched by hand, from small packages, to people, to vehicles, to large shipping containers. The primary disadvantages of manual searches are inconsistent performance of people conducting the searches and slow throughput times.

Random Searches
Random searches may be considered when throughput requirements are difficult to meet with 100% screening.

4.7.1 Metal Detectors

Categories of Metal Detectors
The detection of metal can be divided into two broad categories:

- Active metal detectors transmit electromagnetic energy and detect metal by sensing the response of the metal to the transmitted field.
- Magnetometers rely on the Earth's surrounding magnetic field to detect ferromagnetic materials, which distort the local field.

Methods of Metal Detection: Pulsed Field and Continuous Wave
Two methods are commonly used to actively detect metal, as follows:

- ***Pulsed field detectors*** generate fixed frequency pulse trains in the 400 to 500 pulses per second range. Because of the complex shape of the waveforms used, the pulsed fields may have frequency components from zero to several tens of kHz. Detectors based on this technique represent the large majority of portal metal detectors in use today.
- ***Continuous wave detectors*** generate a steady-state magnetic field within the frequency band of 100 Hz to 25 kHz. While early portal metal detectors were based on this technique they have been largely replaced by pulse portal metal detectors. The majority of hand-held metal detectors are still based on continuous wave technology.

In both cases, the primary reason metal can be detected is the presence of eddy currents (see Figure 11-2). The magnitude of the metal detector's response to metallic objects is determined by several factors: the conductivity of the metal, the magnetic properties of the metal (relative permeability), its shape, its size, and the orientation of the object within the magnetic field.

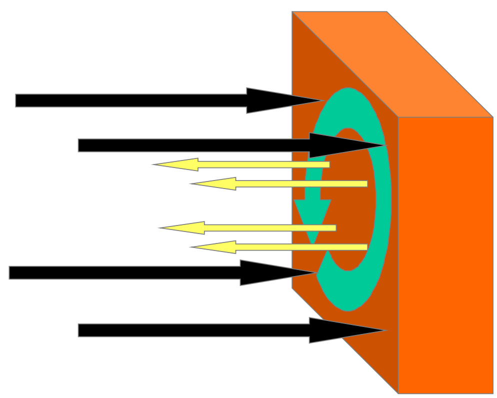


Figure 11-2. When a time varying magnetic field (large arrows) encounters metal, an eddy current (circular arrow) is induced within the metal. The eddy current produces a magnetic field of its own (small arrows) that opposes the original magnetic field.

4.7.2 Continuous Wave Metal Detection Sensors

How the Technology Works
In a continuous wave metal detector, a steady-state sinusoidal signal is applied to the transmitter coil located at one side of the detector arch. This coil produces a magnetic field of low strength (typically 1/2 Gauss or less). The receiver coils are mounted on the opposite side of the arch such that a person being screened passes between the transmitter and the receiver coils. (See Figure 11-3) The signal is detected by the receiver coils and is then analyzed. When there is no metal present within the arch, there is no change in the signal over time.

Eddy Currents Are Affected by Metallic Objects
When a metallic object enters the arch, it alters the magnetic field. The changes in the magnetic field are detected and analyzed. The signal is further amplified and phase detected. If the signal exceeds a selected threshold, an alarm is generated. The phase detection permits some optimization of detection for either ferromagnetic (high relative permeability) or nonferromagnetic (low relative permeability) metals. Figure 11-4 illustrates a continuous wave metal detector.

4.7.3 Pulsed Field Metal Detection Sensors

How the Technology Works
In a pulsed field metal detector, low inductance transmitter coils are used to produce bursts or pulses of magnetic energy typically short in duration (as short as 50 microseconds), 200 to 400 times per second. During the time that the transmitted field is present, the received signal is ignored. Following the end of the transmitted pulse, the received signal is analyzed for a short time (typically a few tens of milliseconds). When there is no metal present in the arch, the output of the receiver is only the background electromagnetic noise (which hopefully is very low). When there is a metallic object present in the arch, the collapse of the magnetic pulse induces an eddy current in the metal. This eddy current decreases rapidly (as a function of resistivity of the metal) but persists long enough to be present when the received signal is analyzed. The signal is then further amplified and phase detected. If the signal exceeds a selected threshold, an alarm is generated. This type of metal detector is by far the most common type of portal metal detectors in use. Figure 11-5 illustrates the operation of a pulse metal detector.

4.7.4 Magnetometers Metal Detection Sensors

How the Technology Works
While the term "magnetometer" refers generically to all metal detectors, an actual magnetometer is a specialized device that is used only sometimes for detection of ferromagnetic weapons and other ferromagnetic contraband. "Ferromagnetic" is a scientific term that means that the material has a relative permeability greater than one (this means that the material is attracted to a magnet). The contraband detection magnetometer relies on the Earth's magnetic field. Ferromagnetic materials that are near the receiver of a magnetometer distort the local magnetic field. Any perturbation of the local field is detected by the magnetometer. The signal is processed and if it is sufficient in strength, an alarm is generated. Figure 11-6 illustrates the operation of a magnetometer.

Factors That Influence Metal Detector Response
In general, for active metal detectors, the main detection mechanism is the presence of eddy currents. Any factor that influences the magnitude of the eddy current will affect the magnitude of the metal detector response. The magnitude of the eddy current depends on the time rate of change of the inducing magnetic field and the resistance of the conductive path within the metallic object. The higher the time

rate of change of the inducing magnetic field, the greater the magnitude of the eddy current. The lower the resistance of the conductive path within the metal, the greater the magnitude of the eddy current. Factors that affect the rate of change for the inducing magnetic field include:

- the orientation of the metallic object,
- the size of the object,
- the ferromagnetic properties of the object, and
- the shape of the object.

The type of metal and the shape of the object determine the resistance of the object and affect the rate of change of the magnetic field inside the conductive path of the object.

Factors that Influence the Rate of Change for the Inducing Magnetic Field

While the orientation of a metallic object cannot influence the time rate of change of the inducing magnetic field within the entire metal detector, it can influence the rate of change within the object itself. tThe orientation of an object can cause more or less magnetic field to strike the object. For example, when the object has its narrowest edge presented to the magnetic field, only some fraction (let us say half) of the magnetic field strikes the object compared to when the broadest surface is perpendicular to the magnetic field. In this example, the time rate of change for the field that strikes the surface of the object is only half as great as when the object is in the orientation that presents the greatest surface area to the field. The more inducing field that encounters the surface of the object, the greater the eddy current and the greater the response.

Ferromagnetic Properties

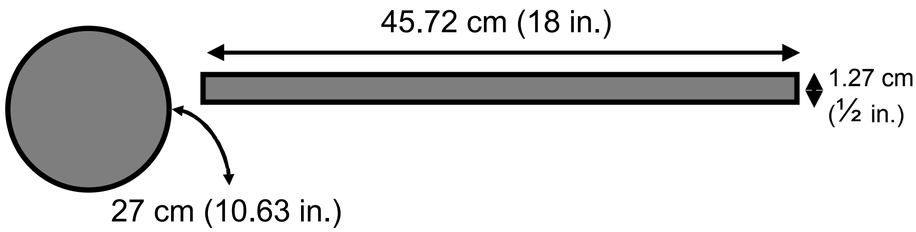
Other factors that affect the time rate of change of the local field that strikes the object are the ferromagnetic properties of the metal from which the object is composed. Ferromagnetic materials actually distort the local field, which has the effect of concentrating the local field (this is the reason transformers often have iron cores). The higher the field strength that strikes the object, the higher the eddy current and thus the easier it is to detect the object.

Factors that Impact the Resistivity of the Object

Another contributing factor in determining the magnitude of eddy currents in a metallic object is the electrical resistivity. The higher the resistivity, the lower the eddy current and thus the harder to detect the object. One obvious cause of the resistivity of the object is the material of which it is made. All metals conduct electricity. Electrical resistivity is the property of a material to resist the flow of electricity. The following table lists some common metals and their electrical resistivity, from least resistive to increasingly greater resistivity. All resistivities are relative resistivities (as compared to copper). Titanium would be the most difficult material to detect of all the metals listed. When the ferromagnetic properties are taken into account, the detectability of the object is much more difficult to predict. See Table 9-1

Shape

Shape also helps to determine the resistance of an object. Electrical resistivity is the intrinsic property of a material but resistance is a property of an object. The resistance of an object is the electrical resistivity of the material of the object multiplied by the length of the electrical path around the object. The following example helps illustrate this role. (See Figure 11 9.)



Both the circle and the rectangle have the same area. The conductive path around the circle is 27cm (10.6in.) while the rectangle has a conductive path that is 94cm (37in.).
This means that the circle will be more detectable in a metal detector.

Figure 11-9. The conductive paths around two shapes made of the same material are different lengths. The path around the rectangle is over three times longer; therefore, the resistance of the rectangle's path is more than three times higher. The response of a metal detector to the circular shape will be three times higher than for the rectangle.

Nearby Metallic and Electrical Devices Can Cause Alarms

The environment surrounding a metal detector can affect a metal detector's performance, as follows:

- Moving metallic objects such as metal doors can cause false alarms even when more than a meter (3 feet) away.
- Static metal objects can also cause problems by distorting the magnetic field and creating areas of high or low sensitivity.
- Electrical devices operated in the vicinity of a metal detector can have adverse effects. Radios, X-ray machines and computers can cause false alarms.
- Metal reinforcing rods in the floor can cause problems. (Pipes carrying water close to the metal detector have caused false alarms. Most likely, the water was causing the metal pipes to move within the walls or floor rather than the detector responding to the moving water.)
- The floor that supports the metal detector needs to be strong enough to minimize bouncing when people walk through the area. Motion induced into the metal detector arch from floor movement may cause unwanted alarms.

In general, any metal (moving or stationary) or electrical equipment operating near the metal detector should be viewed with suspicion when problems occur.

Metal Detectors Used with Nuclear Material Detectors

Metal detection can be an important component of nuclear material detection, specifically to detect metal that can be used to shield the gamma radiation.

Hand-Held Metal Detectors

Hand-held metal detectors have to be operated very close to the person being scanned. At the normal operational distance from the body they are highly sensitive and can be used to find much smaller objects than those that can be found by a portal detector. The effectiveness of a hand-held metal detector is highly dependent on the technique used by the person doing the screening. A hand-held detector in the hands of a screener using careless techniques or using a poor procedure can be very ineffective. On the other hand a dedicated individual following a well designed procedure can be very effective but the process will take a considerable amount of time. Because of the time it takes to use a hand-held detector properly and the short time it takes for a person to pass through a portal, hand-held detectors are mostly used to resolve portal metal detector alarms. In this case the hand-held is used to locate the causes of the alarm in the portal. With this important secondary role every screening point with a portal metal detector should also be equipped with a hand-held detector.

4.7.5 Package Search

Technologies Used for Package Searches
Packages may be searched for contraband manually or by active interrogation. Active interrogation methods used to detect various objects considered to be contraband include:

- single-energy transmission X-ray
- multiple-energy transmission X-ray
- computed tomography (CT) scan
- backscatter X-ray

In general, transmission methods are not safe for use on personnel because of the amount of ionizing radiation; however, a backscatter X-ray technology for screening personnel will be discussed in a later section. In general, single-energy transmission X-ray imagers are used to find metallic items (weapons), while dual energy and backscatter x-ray techniques are designed to image materials with low atomic numbers (low Z). Examples of low-Z contraband materials are explosives, drugs, and food.

Limitations of Single-Energy Transmission X-ray Package Search Systems also gamma interrogation method term usage MARK: to develop - Add section for vehicle search and limitations.
A conventional single-energy-transmission X-ray package search system will not penetrate heavy materials sometimes used for shipping containers. Single energy systems cannot determine the effective atomic number of the material being screened. Because most of the development of low-Z screening devices is directed toward the detection of explosives, these technologies are discussed in detail in the section on bulk explosives detection.

Vehicle Search Systems
Screening vehicles, cargo trucks, and large cargo containers requires higher energy interrogating radiation than is common for small package search systems. X-ray systems with energies of 320 and 630 keV are used for vehicle searches and have been demonstrated to penetrate 10cm of iron. Gamma radiation is also used for interrogation in some vehicle screening systems, using nuclear materials like Cs-137 (661 keV) and Co-60 (1173 and 1333 keV), to provide the radiation which is even more penetrating than the x-ray systems. These high-energy systems, x-ray or gamma ray, require occupants to be out of the vehicle during screening.

4.7.6 Explosives Trace Detectors

Screening Personnel Requires Human-Friendly Equipment
Methods commonly used for inspecting cargo and luggage for explosives (e.g., X-ray imaging or neutron activation), are unacceptable for screening personnel because the ionizing radiation is harmful to humans. Passive detection techniques can be used safely to search personnel or packages for explosives by detecting the trace amounts of vapor that is emitted from:

- bulk quantities of concealed explosives or
- surfaces contaminated by persons who have handled explosives or where explosives have made contact.

The challenge involved in detecting trace explosives is evident when one considers the low vapor-phase concentrations of several common high explosives (see Table 11-2). Concentrations in the parts-per-billion or parts-per-trillion range are typical, with further reductions in vapor pressures encountered when the explosive constituent is packaged in an oil-based gel or solvent (e.g., RDX in C-4 plastic explosives).

Table 11-2: Vapor Pressure of Explosives Molecules at Room Temperature and Atmospheric Pressure

Explosive	Constituent of	Vapor Pressure (parts per billion)
ethylene glycol dinitrate (EGDN)	Dynamite	92,000
nitroglycerin (NG)	Dynamite	340
dinitrotoluene (DNT)	Military TNT	300
trinitrotoluene (TNT)	Military TNT	8
cyclonite (RDX)	C-4, Semtex	0.006
pentaerithrytol tetranitrate (PETN)	Detasheet, Semtex	0.002

Collection of Explosives Vapor Is Difficult
Explosive molecules also readily adsorb upon most materials at room temperature, and decompose upon moderate heating or upon exposure to large doses of energy. Hence, transport and collection of vapor-phase explosive molecules is achieved only at the expense of significant sample loss.

Methods of Trace Explosives Detection
Several approaches have been developed for the trace detection of explosives. These passive methods of detection are:

- Canine
- Trace detection instruments
    - Ion mobility spectrometry (IMS).

Using Dogs to Detect Explosives
Canine (See Figure 11-10) has been used widely in the police and military for locating hidden explosives. However, canines require constant retraining to continue to identify synthetic compounds such as explosives. Moreover, the reliability of canine inspection is subject to the health and disposition of the dog and the vigilance and skill of the handler. Canines are usually trained on 6-10 odors. For these reasons, commercial explosive detectors are gaining greater acceptance as the preferred method for screening personnel for explosives.

Figure 11-10. Canines Are Used to Detect Explosives and Other Chemical Compounds

Ion Mobility Spectrometer Detector
In an ion mobility spectrometer (IMS), the analyte molecules in the air sample are ionized negatively using a beta source. The ions then pass into a drift region through a shutter that opens periodically over millisecond intervals (see Figure 11-11). Within the drift region, the molecules separate by weight, with the lightest molecules progressing more quickly than the larger molecules. At the end of the drift region, the ions strike a Faraday plate, which records the output current as a function of molecule drift time. A typical IMS drift cell is 6 to 8 cm in length with an electric field gradient of 200 V/cm. Under these conditions, the drift times of the explosives molecules range from 5 to 20 milliseconds.

IMS-based Detectors
IMS-based detectors provide high sensitivity to dynamite, military-grade TNT, and plastic explosives compounds, at instrument costs that are considerably lower than those of chemiluminescence detectors. The sensitivity of the IMS-type detector and its relative ease of operation and maintenance account for the rapid development and commercialization of IMS technology for explosive detection applications. Because IMS instruments can detect very small masses (nanograms) of some explosives, it can be challenging (10-30 minutes) to clear explosives residues out of the instrument after a large detection.

Surface Sampling (Swipe) Mode
Most commercial explosives detectors achieve greatest sensitivity when used in the surface sampling mode, in which a surface suspected of explosives contamination is swiped with a collection substrate. The collection substrate is then placed in a heating unit, which desorbs the particles of explosives that have been gathered, and transports them to the detector for analysis. Swipe modes are impractical for high-throughput areas because of time constraints.

Walk-through Personnel Portals
For screening individuals passing through sensitive high traffic checkpoints, such as airport boarding areas, several walk-through personnel portals have been developed for screening high throughput areas for explosives.

Factors to Consider for Selecting Explosives Detection Equipment

Commercial explosives trace detectors must be carefully selected to meet the needs of each facility. Factors to consider when selecting an explosives detector include:

- sensitivity
- types of explosives detected
- false and nuisance alarm rates
- time required to warm up and operate
- initial costs
- operating and maintenance costs

4.7.7 Bulk Detection

Using Characteristics of Bulk Explosives for Detection
Bulk explosives detection devices measure some bulk characteristics of materials in an attempt to detect the possible presence of explosives. Some of the bulk characteristics that may be measured are the X-ray absorption coefficient, the X ray backscatter coefficient, the dielectric constant, gamma or neutron interaction and, microwave or infrared emissions. Further analysis of these parameters can result in calculated mass, density, nitrogen content and, effective atomic number (effective Z). While none of these characteristics are unique to explosives, they are sufficiently unique to indicate a high probability of the presence of explosives. The false alarm rate for bulk detection devices can be low enough to allow for automatic detection of materials that may be explosives. After the system generates an alarm, the human operator can investigate and determine whether or not explosives are present.

Nuclear Technologies
Nuclear technologies interrogate an object using neutrons. Currently the only two commercially available nuclear technology detectors are the thermal neutron activation (TNA) detector and the pulsed fast neutron absorption (PFNA). Thermal neutron devices can determine the nitrogen content of a material. Nuclear absorption of a thermal neutron makes 15N in an excited state from 14N. The excited state is not stable and emits a gamma ray of characteristic frequency. Detection of this gamma ray is then a measure of nitrogen content. Since most explosives are nitrogen rich, these devices can automatically detect their presence. PFNA devices can roughly measure the H, C, O composition of the material. When combined with thermal neutron measurement of N content, a more specific identification of the material is possible. However, PFNA systems are much more expensive than thermal neutron systems. Drawbacks are a high cost size, and throughput. Some package search systems are based on TNA and some systems for searching vehicles and large shipping containers are based on PFNA.

X-ray Technology
In most cases, X-ray technology bulk detectors are modified package search X-ray scanners. These devices usually serve a dual purpose. The package being searched for guns or other contraband is analyzed simultaneously for the presence of materials that may be explosives. Simple single-energy-transmission X-ray scanners do not provide enough information to make automated explosives searches, depending on the operator's interpretation of the image; a method to extract more information is needed. Dual energy allow the determination of a material's approximate mass absorption coefficient. Dual energy (around 80 and 130 keV) measure the ratio of transmitted energy at the two energies, and by comparison with known elemental attenuation coefficents, can measure an effective atomic number for the region scanned. Typically, false colors are added to the images to indicate areas of low-Z and high-Z materials. The colored regions may aid personnel in interpreting the images. Computed tomography scanners can extract enough information to calculate the material's mass, density, and mass absorption coefficient. Backscatter technology can determine a material's effective Z by examining the amount of X-

ray energy scattered back in the direction of the source (a process mainly due to Compton backscatter, most effective for hydrogen-rich materials like explosives, plastics, and food). Giant X-ray systems to screen trucks are available, and an operator still has to interpret the image.

Backscatter Device for Use on Humans

A device is commercially available that uses low energy X-rays at ambient levels to image materials on the bodies of persons being screened. The device can image guns and other contraband including explosives hidden under the clothing of persons being scanned. This backscatter device subjects the subject to about 2.5 microrem per scan. While the energy level is very low and considered safe, many people find any exposure to X-rays objectionable. Also at question is the invasion of privacy issue, because the screened person's body is imaged through the clothes. In the case of detectors that do not have Automated Threat Response (ATR) capability, detection of explosives is not automated; the operator has to view the image to see contraband objects.

Millimeter Wave Imaging
Millimeter wave imaging is a commercially available technology for imaging people. The active electromagnetic radiation is approximately 100 GHz in frequency. Most clothing is transparent at this frequency. The skin reflects brightly. Metals strongly absorb this frequency. Images produced can reveal hidden items like guns, knives, and explosives. The images can be graphic, and some systems conceal private areas or use software (rather than a person viewing the image) to determine detection. Secondary screening, typically pat-down searches, is required to resolve detected anomalies.

4.7.8 Nuclear Material Detectors

Methods of Detecting Nuclear Materials
The purpose of nuclear materials detectors is to detect the unauthorized removal of nuclear materials on persons, in packages, or in vehicles leaving a security area. Methods to detect nuclear materials can be:

- ***Passive***—Passive methods use gamma ray and neutron detection techniques to detect the natural radiations and emissions from nuclear materials. These methods can be defeated by shielding with metallic lead, composite lead materials, or organic shields if the quantity of nuclear materials is very small.
- ***Active***—Active methods use neutron activation or X-ray techniques.
- ***In combination with metal detectors to detect radiation shielding***— When a portal metal detector is used to detect nuclear materials and the materials used to shield them, it must be able to detect relatively small quantities of high atomic number (Z) metal, such as lead. Because the resistance of high-Z metals is generally higher than lower-Z metals, they tend to be more difficult to detect. In all cases, very high sensitivity operation will be required. Because high sensitivity operation will sharply increase the nuisance alarm rate, an area for personnel to change out of steel-toed shoes and to remove other metallic items from their clothes may be required. Hand-held metal detectors can detect very small quantities of metals and may be better suited to the task of screening for nuclear materials. The disadvantage of hand-held metal detectors is the requirement for active guard participation in the screening process and the time required for the search. While portal (and hand-held) metal detectors will detect metallic forms of nuclear materials and metallic shielding, some forms of nuclear materials and other shielding materials cannot be detected by metal detectors.

Detection of Nuclear Materials Employ Several Passive Techniques
Detection of radiation emitted from nuclear materials is accomplished by using one of several detection materials. Scintillators may be crystalline or organic (within a plastic matrix), semiconductor (solid state) detectors conduct electrically when exposed to radiation, and proportional detectors contain gas that can detect neutrons

4.7.9 Gamma Ray Detectors

Scintillators Detect Gamma Rays
Some nuclear materials detectors contain scintillators that detect gamma rays from the radioactive decay of nuclear materials. Scintillation is the process by which photons are produced as a result of the absorption of ionizing radiation in scintillator material. Typically, the detectors are crystalline (sodium iodide) or plastic, the latter being used extensively in pedestrian portals. Because gamma radiation can be

shielded with metal, radiation and metal detectors are usually combined to form an effective screening system.

Crystalline Scintillator
Thallium-activated sodium-iodide coupled to a photomultiplier tube is commonly used to detect gamma rays. NaI(Tl) has become one of the most widely used materials for gamma ray detection. Pure sodium-iodide crystals scintillate efficiently when cooled to around 77 K but lose most of that efficiency when near room temperature. The addition of thallium not only increases the efficiency at room temperature, but also causes a shift in the wavelength of the scintillation light such that NaI(Tl) is transparent to its own scintillations. One drawback is that exposure to small amounts of moisture causes the NaI(Tl) to discolor, thus lowering its transparency to the scintillation light and making it useless for radiation detection. NaI(Tl) detectors have some energy resolution and are somewhat useful for distinguishing between various isotopes that radiate and have no sensitivity to neutrons. Lanthanum bromide ($LaBr_3$) has slightly better resolution than NaI, and is becoming commercially available.

Plastic Scintillators
Plastic scintillators emit photons when high energy rays (x-ray, gamma, neutrons) are incident on the plastic. They cannot discriminate the energy of the radiation that produces the scintillation, thus they cannot identify the isotope detected. The plastic material is much cheaper than the crystalline scintillators described above per unit area. The plastic also has lower efficiency than the crystalline materials per unit area. When the cost and efficiency are combined, plastic scintillators provide more sensitivity at a lower cost, but with the loss of any energy resolution. Providing some neutron detection in addition to gamma detection, they are commonly used for radiation screening of personnel.

Solid State Semiconductor Detectors
Solid state detectors like high purity germanium (HPGe) and cadmium zinc telluride (CTZ) can measure the energy of the gamma ray incident on the crystal. This allows the specific identification of the isotope, because the energy of the gamma emitted is characteristic of the isotopic decay. Such specificity is particularly useful in distinguishing the source of nuisance alarms. For example, a person that has recently had a medical procedure using a radioisotope (like technicium) will present enough gammas to be detected. Solid state detectors can have enough resolution to distinguish the technicium gamma energy spectrum from that of a real threat like U-235. While these semiconductor crystals have excellent efficiency (sensitivity per unit area) and good energy resolution, they are more expensive per unit area than plastic scintillators. The HPGe crystal requires expensive cooling. Germanium-based detectors are often cooled with liquid nitrogen, for example. CZT detectors achieve reasonably good energy resolution at room temperatures. Solid state detectors also have some neutron sensitivity.

Detectors Consider Background Radiation Before Generating an Alarm
Alarms are generated by alarm circuitry that detects when a statistically significant increase over the normal background reading has occurred. Select an alarm threshold close to the normal background level but not so close as to cause a large number of nuisance alarms. The signal count is compared to an alarm level derived from an average background count. The background level is established by making counts over a number of counting time intervals. This reference background count is continuously being accumulated, updated, and averaged. Typically, in commercial walk-through models, the signal count is accumulated only during occupancy. Each time the signal count is updated, it is compared to the alarm level, and an alarm occurs if the signal count exceeds the alarm level. Other alarms detect power line failure, equipment failure, excessively high or low background, or equipment tampering.

Detectors with fair to good energy resolution can eliminate potential sources of nuisance alarms from the background.

Handheld Detectors and Vehicle Searches
Hand-held detectors are available for searching people, packages, and vehicles. Equipment can be installed in vehicle portals to provide automatic detection. (See Figure 11-13.)

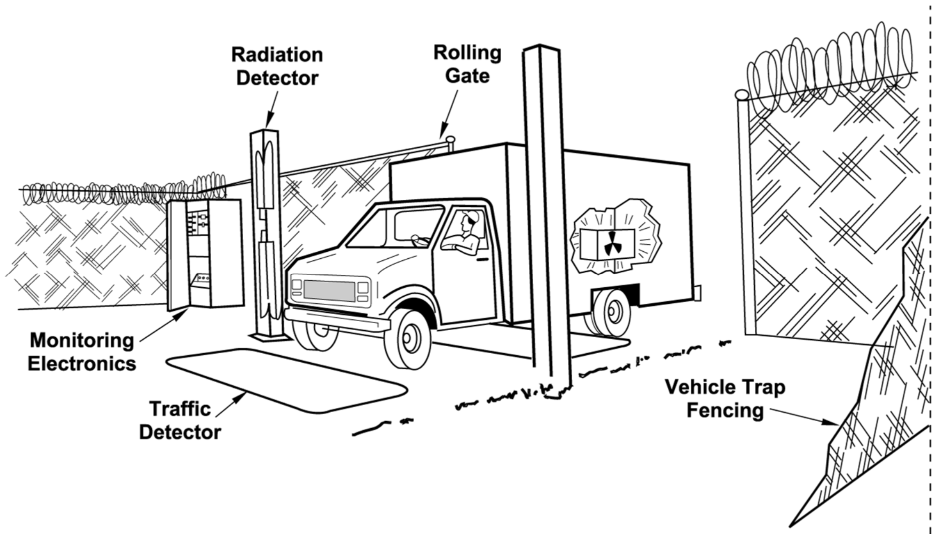


Figure 11-13. Vehicle CATEGORY 1 Monitor Portal

4.7.10 Passive Neutron Detectors

Neutron Detectors
Neutrons can be detected using materials that capture a neutron and produce a detectable particle, for example ^3He or BF_3 sensors. The energetic ion (alpha or proton) is then detected.

$$^{3}He + {}^{1}n \rightarrow {}^{3}H + {}^{1}p\,, \quad 0.76\ \text{MeV}$$
$$^{10}B + {}^{1}n \rightarrow {}^{7}Li + {}^{4}\alpha\,, \quad 2.3\text{-}2.7\ \text{MeV}$$

Neutron detection is attractive when monitoring for nuclear material because some of these materials (especially plutonium) emit neutrons, shielding neutrons is difficult, and because the neutron background is generally very low. Thus, neutron detectors can be very sensitive and the detection of neutrons is a good indicator of the presence of nuclear material.

5. Evaluation of PPS Effectiveness of a Nuclear Facility –

5.0 Evaluation
A physical protection design is considered to be effective if it meets regulatory requirements as specified by the Competent Authority. Generally, these requirements fall into three categories:

- Prescriptive requirements: Are base-line measures in place? As examples, "a 2.4 meter chain-link fence is required on the boundary of the limited access area" and "an approved security plan will be in place."
- Prescriptive requirements with performance requirements: Are baseline measures in place and are they acceptance-tested and maintained according to standards specified by the Competent Authority as meeting the intent of the regulatory requirement? "As an example, a perimeter sensor should provide a high assurance of adversary sensing as defined in standards that it provides probability of sensing of 90% with 95% confidence."
- Systems-level performance-based requirements: Are measures in place that are effective against adversary capabilities as specified in the threat assessment or DBT? As an example, "the PPS should demonstrate a Probability of System Effectiveness of .93 or better against the DBT."

The design should meet these regulatory requirements across the range of facility or transport operations and states in a graded fashion to match the theft or sabotage targets found at the facility or the range of transport operations.

The evaluation should also consider design issues that may be associated with regulatory requirements such as:

> Does the system provide a high assurance of operating effectively during an adversary attack, considering redundancy and diversity of physical protection measures as well as the implementation of compensatory measures?

Some design issues are not necessarily associated with meeting regulatory requirements:

- Does the system provide defense-in-depth across a series of protection layers, taking into account the combination of technical measures and administrative measures such as protection of sensitive information?
- Does the PPS provide balanced protection across adversary scenarios for the variety of operational states?

The latter issue is important in its own right: a system may meet regulatory requirements but provide imbalanced protection. Where this is true, the designer may be able to reduce system capabilities where they clearly exceed requirements, thereby reducing the initial and/or operational costs of the system.

It is an implicit aspect of good design that technology and administrative measures are selected and implemented in such a way that they operate properly and are cost-effective.   Competent designers do not typically select the use of a certain type of biometric identification and then plan to operate it in a degraded mode. Thus, any system design that has such flaws should be re-engineered before it reaches the evaluation phase.

By way of comparison, the evaluation phase of design is meant to:

- Determine whether the design "is good enough" to meet regulatory requirements and to improve it by increasing effectiveness where it falls short while removing capability where it significantly exceeds regulatory requirements; and/or

- Compare the effectiveness of several design options to support selection of the best option.

Such comparisons are particularly valuable during conceptual design.

5.1 Overview of evaluation process

During the evaluation phase, the PPS design, whether it is a new or existing system, is evaluated to determine whether it meets both regulatory and derived requirements identified earlier. In the evaluation phase, data are collected (see "Performance Testing" in Figure 2 – Process for developing the PPS Design), and then Path Analysis and Scenario Analysis are performed on the design as part of overall system evaluation (see section 5.4). As the design becomes more detailed, personnel training to plans and procedures need to be evaluated (see section 5.3).

The evaluation process is slightly different depending upon whether performance requirements exist in addition to prescriptive requirements.

5.1.1 Meeting Prescriptive Requirements, Including Those with Performance Requirements

As described in NST 025, "In the prescriptive method, the State establishes specific physical protection measures to meet its defined physical protection objectives for each category of nuclear material and each level of URC. These measures provide a set of 'baseline' provisions for the operator to apply for each category of material and each level of URC. The Competent Authority can also impose prescriptive requirements also to mandate a particular design approach or design solution. For example, mandating that perimeter detection must include a fence with at least two sensors ensures a specific design approach for this PPS component. Prescriptive requirements are often used where compliance with higher level policy is necessary, or where it is more efficient to ensure a common design of a component across the physical protection regime.

Virtually all physical protection systems will have some prescriptive requirements; so typically a PPS design will be checked against this type of requirement. Prescriptive requirements for a design will be verified before there are systems-level performance requirements as the latter requirements are much harder to validate.

Prescriptive requirements typically focus on individual physical protection measures or subsystems. As such, evaluation methods consider whether those measures or subsystems meet baseline requirements, which may include performance requirements. Such performance requirements may consist of:

- Probability requirements such as providing probability of sensing or detection of 90% with 95% confidence (quantitative) or high assurance of detection (qualitative);
- Delay requirements: certain barriers should provide at least X minutes of delay against all adversary tools and equipment as specified in the DBT; or
- Response requirements: arrival of N responders who meet training and weapon requirements within Y minutes.

Several aspects of the DBT/TA are important from the perspective of designing physical protection components and subsystems to meet performance requirements:

- Numbers of adversaries: this will affect derived response requirements[1] necessary to interrupt and neutralize the adversary and, to a certain extent, affect delay times and probabilities;
- Weapons: this will affect derived response requirements in terms of response times, training and equipment and, to a certain extent, delay times (as weapons may be used to penetrate barriers);
- Explosives: this will affect derived delay requirements and may affect derived response capabilities where such explosives may be used to degrade response capabilities;
- Tools: these will affect derived delay requirements (such as delay times) and the ability to meet derived probability requirements (as tools may enable the adversary to spoof or bypass sensing or assessment capabilities);
- Modes of transportation: this will affect derived delay requirements for vehicle barriers and standoff requirements (as determined by explosives capabilities against target) and, to a certain extent delay requirements against barriers in general (as vehicles can be used to bring equipment closer to the target);
- Technical skills (such as ability to use explosives and to defeat targets) and knowledge about the facility/transport operation and physical protection system: these can affect derived detection, delay, and response requirements;
- Insider threat issues (including active/passive involvement and access, authority, and knowledge of different categories of insider): these may affect derived detection, delay, and response requirements;
- Adversary tactics: this may affect derived detection, delay, and response requirements according to the adversary capability to use stealth, deception/deceit, or force.

The ability of components and subsystems to meet such performance requirements may be verified at various phases of design, construction, commissioning, and operations based on technology testing, performance tests, and exercises (to include Force-on-Force exercises). These topics are covered in sections 5.2 and 5.3.

Some physical protection component and subsystem requirements are conceptually linked to their ability to counter threat capabilities but are not practically approached that way during design. As an example, requirements for tamper-protection are prescriptive because it is hard to collect sufficient information about the threat to determine how easily an adversary from DBT can defeat line supervision, Tamper-Indicating Devices, or tamper switches on hardware. Requirements for test items for metal detectors also fall in this category. These prescriptive requirements may, however, be developed based on insights gained during testing.

5.1.2 Meeting Systems-Level Performance-Based Requirements

The PPS system-level objective is to prevent a successful adversary attack on a protected asset. Systems-Level performance requirements are defined, conceptually, in terms of the probability that the physical protection system will defeat the adversary before an adversary attack can achieve its theft or sabotage objective. This probability requirement can be specified quantitatively (e.g., in terms of Probability of System Effectiveness, P_E, such as "$P_E > .3$") or qualitatively (the PPS will defeat the adversary with high assurance).

---

[1] A derived requirement is a physical protection specification deduced from regulatory requirements as part of the design.

A PPS has certain inherent system functions[2] which operate to achieve the system level objective. Integrating these functions effectively is the focus of PPS engineering and system development. At a systems level the physical protection system is effective if that system detects, interrupts, and neutralizes the adversary. As defined in the NST023 implementing guide:

- *"Interruption begins with communication to the response force and is completed when a sufficient number of appropriately trained and equipped members of a response force arrive at the appropriate location in time to stop the adversary's progress towards completing a malicious act."*
- *Neutralization is the act, following interruption, of gaining control of the adversary before their goal is accomplished or otherwise causing the adversary to abandon the attempt."*

Based on these definitions, the Probability of System Effectiveness, PE takes on the form:

P_E= Probability of Interruption * Probability of Neutralization (given interruption) = $P_I * P_N$.

P_N is a conditional probability, measuring the probability that the PPS defeats the adversary given that interruption occurs. To be complete, the evaluation process needs to cover two types of questions:

- How does system effectiveness vary across the variety of adversary tactics, facility operational states, adversary capabilities, PPS protection layers, and routes taken by the adversary into the facility?
- Given a detailed adversary attack, how well does the system perform (that is, what is PE qualitatively or quantitatively)?

Path analysis partially answers the first question by looking across a variety of factors to determine whether there are weaknesses or not; whether performance requirements seem to be met, at the resolution used in the analysis; whether there is defense in depth, and whether there is balanced protection. The theoretical basis for path analysis is the inequality

$$P_E \leq P_I.$$

Thus, if P_I is low then P_E will also be low. To simplify the problem, path analysis determines conservatively low estimates of P_I; the design is not considered to be sufficient unless these conservative estimates are sufficiently high[3].

An adversary path is an ordered series of actions against a target which, if completed, results in successful theft or sabotage. A description of a path includes both information about where the adversary physically goes within the facility and the tactics used by the adversary against different parts of the PPS encountered along the path.

Path analysis determines P_I over the set of adversary paths used to attack facility targets and identifies those (most-vulnerable) adversary paths having the lowest P_I. The effectiveness of the resulting PPS design is taken to be P_I for the most-vulnerable path(s). If P_I is inadequate along the most-vulnerable path(s) then the PPS design will be considered inadequate.

---

[2] Function - A defined objective or characteristic action of a system or component. (IEEE 610.12-1990)

[3] As an example, if the regulatory requirement is that P_E is greater than or equal to .3, then the designer could require all of the conservative P_I estimates to exceed some value greater than or equal to.3.

Path analysis can also provide insight into whether there is defense-in-depth by considering those physical protection measures that provide timely detection to P_I as well as those elements that provide delay along the adversary path. Finally, path analysis can also examine whether protection is balanced by describing how P_I varies across the set of adversary paths against a target. The models used to describe all of these paths, such as Adversary Sequence Diagrams, can also provide information about how well delay and detection capabilities are balanced across different boundary elements, such as doors, walls, and fences, surrounding a specific security area, be it a protected, inner, and/or vital area.

With its focus on interruption, path analysis is especially useful for identifying those technical deficiencies in the PPS design that might prevent effective interruption of the adversary through their effects on adversary delay times, detection probabilities, or PPS response times.

The effect of certain aspects of the DBT/TA, such as the assumed set of adversary tools and explosives, can be also be studied through path analysis where these factors have a direct influence on P_I through their effect on adversary delay times or detection probabilities or PPS response times. On the other hand, the fidelity and conservatism of path analysis can significantly limit understanding of how other factors, such as the selection and type of response weapons or specific response tactics, techniques, and procedures or the effectiveness of training, will affect probability of neutralization in particular or P_E more generally. Such factors are considered during path analysis only to the perhaps limited extent to which they indirectly affect detection probabilities, delay times, and PPS response times.An adversary attack, as well as the resulting response, is ultimately conducted by human beings; therefore, to fully determine PPS effectiveness, human actions must be examined directly, and this is done by means of scenario analysis.

Scenario analysis addresses the second type of question: Given a detailed adversary attack how well does the system perform (that is, what is P_E qualitatively or quantitatively)? Scenario analysis can only address a limited number of scenarios out of the space of all adversary scenarios but if the scenarios are selected carefully these can provide insight into system effectiveness. The determination of P_E requires more detailed information about the response forces, the threat, and the PPS, as well.

5.2 Performance Testing

As defined in NSS-13, performance testing is defined as "*Testing of the physical protection measures and the physical protection system to determine whether or not they are implemented as designed; adequate for the proposed natural, industrial, and threat environments; and in compliance with established performance requirements.*"

Certain types of performance testing, such as force-on-force exercises, can only be performed on an existing physical protection system at an actual nuclear facility; this section will focus on tests performed on physical protection measures and subsystems.

Several types of performance tests can be identified:

- Tests of technical measures to study their fitness for specific natural or industrial environments or their ability to comply with established quantitative and/or qualitative performance requirements;

- Tests to determine how technical measures and subsystems may be defeated (these may be used to support fault tree analyses to understand comprehensively how those measures and subsystems can be defeated);
- Tests to determine performance metrics (such as detection probabilities and delay times) representing how well technical measures and subsystems perform against attacks performed by adversaries with varying levels of capabilities, to include the DBT/TA.

Technical measures are typically tested at specialized testing facilities that use rigorous methods to study the fitness of such measures in various operational environments. Such facilities are also used to determine maintenance tests and procedures. Defeat testing of technical measures and subsystems can also be performed at such testing facilities wherever practical. Such tests provide the data required to develop barrier delay times for specific barriers.

In some cases, the tests need to be performed at the nuclear facility's site itself. Such tests might be performed before the facility construction is completed (for example, when sensors are tested to determine whether they work acceptably in a particular environment) while others occur when the facility is acceptance-tested or later during operations.

PPS evaluation, by definition, is evaluation of data. The methods and programs by which that data is gathered, analyzed and managed directly influence the validity of the PPS design's evaluation. The planning and conduct of performance testing can require a significant investment of resources. Security program managers should implement performance testing programs that make use of ongoing testing conducted by site maintenance personnel, security force trainers, as well as dedicated PPS testing to make efficient use of available data.

5.2.1 Elements of a Performance Testing Program

A Performance testing program include these elements:

- Coordination and Planning. To integrate available data from other testing programs, such as maintenance and training, there should be coordination with other testing programs to integrate testing objectives and methods to maximize the utility and relevance of test data. A planning activity should ensure the preparation of resources and the integration into site operational schedules to minimize disruption. Test activities should be documented in a test plan that establishes the objectives, standards, methods & procedures by which testing will be accomplished.
- Test Design and Conduct. Performance tests should be designed to test performance against requirements. Performance tests should be designed to obtain sufficient data to support quantitative evaluation of performance with an appropriate degree of statistical confidence. The conduct of performance testing should be done with trained personnel trained in the operation of the PPS element, and the appropriate procedures established in the test plan. Performance testing should be accomplished by impartial test personnel to ensure accurate data.
- Data Management. There are several attributes of performance test data that are important to understanding how the data can be interpreted and used. These attributes should be identified and documented in a data management plan to guide the effective collection and maintenance of performance test data. Examples include:
    - *Context* – why was the data collected? For example, it might have been collected by site maintenance personnel to support maintenance trends reporting.

- *Age* – when was the data collected? The age of the data may affect evaluation of its relevance to the current PPS.
- *Data structure* – to use data collected from several sources and activities, there should be a common structure of metrics. For example, data associated with detection sensors could include ranges at which sensing occurs, nuisance alarm rates, numbers of false positives and negative sensing events. This structure should specify a common organization of metrics so that they can be easily aggregated. Terms and definitions should also be specified in a data structure.

5.2.2 Best Practices for Performance Testing

- Performance test plans should outline the following:
    - Test objectives,
    - Conditions under which the test will be performed,
    - Relevant standards, requirements and technical references
    - Quantitative method that will obtain sufficient required data
    - Specific test procedures that will guide the performance of the test
    - Specification of the test article; for example, its make, model, version number and other attributes that will assist in comparing this test to other tests of similar components.
    - Results of the test and the supporting data
- Performance tests should be repeatable and impartial. To be valid, additional testing by different sets of experts using the same test plan should yield comparable results.
- Test design should be well structured to ensure the most efficient and accurate use of individual test trials and observations. Use of established international standards, such as ISO/TC 69, Applications of Statistical Methods, provide additional best practices in the appropriate use of data sampling and design of experiments.

5.3 Evaluation of personnel, plans and procedures, including protection against insiders

A physical protection system integrates the PPS components of people, plans, procedures, and equipment for the protection of assets or facilities from unauthorized removal of nuclear material and/or sabotage. Validation of the system effectiveness of the physical protection system requires that all PPS components of personnel, plans, procedures, and equipment be performance tested, analyzed, and inspected to ensure that the system effectiveness is maintained at the State defined level which provides an acceptable level of protection for all targets against all threats.

Determining which PSS to test is usually based on information uncovered during document reviews, interviews, and data collection activities. If this information leads evaluators to think that a weakness may exist along a particular adversary path, or if the maintenance history of a system indicates a potential weakness, the systems identified with these weaknesses should be tested.

Evaluation of the PPS component effectiveness should be performed in all phases of the PPS from design to operational turnover to daily functional testing. As a component is incorporated into the PPS the system effectiveness it should be tested from inception throughout its lifecycle. There are a number of performance-based methods available such as Path Analysis, Simulation, and Exercises. Exercises range from Force-on-Force exercises which test the complete PPS, training and readiness of a response force to Limited Scope exercises which test components of the PPS. All physical protection measures including technical, procedural, and administrative provisions should be tested, reviewed, and evaluated. Limited Scope exercises can be used to evaluate the use of security measures such as technologies, plans, procedures, training and qualification of operational personnel, security specialists and guards.

When evaluating key components of the PPS, insider attributes should be considered. The insider can utilize their access authorization, authority and knowledge to bypass dedicated physical protection components or other provisions such as procedures. Insiders can select the most vulnerable target and the most opportune time to perform the theft or sabotage. The insider may also employee protracted theft where the insider extracts small amounts of nuclear material for several days or weeks until the insider has amassed a goal quantity of nuclear material.

To aid in defending against the insider threat the physical protection system is assisted by nuclear material accounting and control measures, process controls, safety alarms, operational alarms, and observations by co-workers or supervisors. When evaluating the effectiveness of the PPS all of these components should be tested as well.

The overall approach consists of implementing several layers of defense, including both administrative aspects (procedures, instructions, administrative sanctions, access control rules, confidentiality rules) and technical aspects (multiple protection layers fitted with detection and delay) that insiders would have to overcome or circumvent in order to achieve their objectives. (NSS08, 5.2). Some of these measures are associated with protective layers around security areas, such as Protected Areas, Inner Areas, and Vital Areas; in most cases, such measures are provided by humans or by capabilities within areas.

Personnel

There are a variety of methods to evaluate the performance of personnel who perform PP activities. During any evaluation process it is best to use multiple techniques to determine personnel assigned to PP activities are successfully performing their assigned PP function. Evaluation methods include direct observation, interviews, job knowledge testing, and limited scope performance testing and full exercises.

The evaluation of PPS preventive measures to defeat the insider may include, review the operator programs for personnel identity verification, trustworthiness checks for initial and ongoing access to the facility and to information concerning it; escorts and surveillance of infrequent workers and visitors, and security awareness training for all workers. The evaluator should also review the operator employee satisfaction program to ensure it fosters good relations between workers and management and that workers are given due consideration and should be part of the security culture.

Plans

Any evaluation of the PPS should begin with a review and evaluation of operator nuclear security plans. Documents to be reviewed include:

- Operator nuclear security management structure/charts
- Operator nuclear security plans and procedures

- Operator transportation plans and procedures
- Listing of waivers and exceptions
- Past survey reports and inspection reports
- Facility asset list
- Maps/drawings showing security areas, buildings, Protective Force posts, vital equipment areas, and NM storage areas. PPS plans may include compartmentalizing the facility using a comprehensive network of access control; and safety provisions

Given that the information contained within it would be of great value to an adversary, steps should be taken to ensure the confidentiality of the physical protection plan. Access to the detail in the plan should be limited to those with a definite need to know to ensure confidentiality (security of information).

Procedures

Records and procedures should also be evaluated for completeness and accuracy. Records include:
- Operations logs and test records;
- PSS maintenance, testing, and repair records;
- Trend analysis information;
- Occurrence reports;
- Force-on-force after-action reports
- Protective force post orders,
- PPS maintenance procedures,
- MC&A procedures, and
- Facility operating procedures;

Typical evaluations verify whether:
- PSSs are accurately characterized in VAs and security plans.
- Response times are consistent with those identified in security plans.
- Equipment is tested and calibrated according to traceable specifications.
- Procedures are complete and describe the actual methods of operation.
- Personnel adhere to procedures in performing their activities.
- Personnel are knowledgeable of their duties and responsibilities.
- Equipment is in good repair.

5.3.4 Protection Against the Insider

The Security Plan should describe the Insider Mitigation Programme's principles. All insider mitigation policies, procedures/plans are subsequently, designed and established per the principles. Policies define site specific rules for meeting the principles/requirements. For example, the site may decide that the requirement for identity verification at the Protected Area Boundary will be met by using finger vein biometric. Policies will also result in establishing design constraints and thus become derived requirements. Polices will also evolve as the design matures.

A systematic evaluation process should verify that all procedures – independently and as part of an integrated system – meet design objectives identified in the Insider Mitigation Programme as well as verify effective performance by the individuals and equipment implementing the procedure.

The evaluation should start by understanding the security strategy wrt given requirements as well as the derived requirements (understand the constraints that are the result of design decisions). Plans and procedures should be evaluated using a two-fold approach:

1) Does the plan/procedure meet the purpose, intent, and/or requirement?
2) Has the procedure been effectively implemented? – do the actions identified satisfy the stated purpose and intent.

For the insider adversary, a review of the written procedures should ensure that the measures are effectively implemented, specifically reviewing:

- the site's process for justifying and authorizing access, including identification of personnel who can and cannot authorize access
- the process for determining compartmentalization of areas and segregation of duties AND how the results of the determination are implemented and controlled.
- Surveillance procedures, including reporting
- The types of data and other evidence that may need to be captured for investigation and final assessment
- mechanism(s) for reporting of irregularities
- How procedures address different facility operations and conditions such as:
    - Normal operations,
    - Off-normal operations
    - Security incidents
    - Safety incidents
    - New condition/processes

The process for evaluating implementation of the procedures may include:

- observation (behavioral-based evaluations) of individuals performing procedures[4], including performance testing of anomaly identification
- performance testing equipment used in the procedure
- audits of logs and other data generated by procedures

An insider mitigation program is developed using a top down approach, starting with defining principles for insider protection, then developing policies consistent with these principles, and finally developing procedures consistent with the policies. Policies help define the protection strategy by defining the aims and goals of the protection system. Procedures define processes and specific operations required to implement the policies.

Principles are typically defined early in the requirements phase; policies and procedures are usually defined and refined throughout the design and implementation process. Thus, this development process inherently considers implementation of alternative measures.

[4] Note that the evaluation is intended to validate the understandability and interpretation of the procedure and should not be a reflection on the individual. This is different than identifying a blatant procedural violation – a reportable incident – during normal conduct of the procedure.

The decisions behind the preventive measures implemented (and those that weren't) should be understood and documented. These measures are evaluated prior to implementation, therefore, the required level of detection required for specific protection measures should be determined as part of the design and implementation process. The evaluation of protective measures (that is detection, delay, and response measures) against the insider should not implicitly assume, through grouping insiders for example, that measures are in place to prevent individuals from gaining authorized access to designated security areas, but should ensures the measures have been reviewed against regulations and are implemented effectively.

5.4 Overall System Evaluation

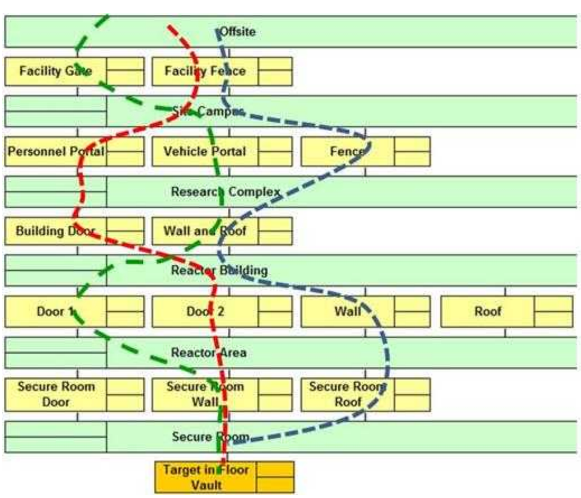
5.4.1 Path analysis

As discussed in NST023, path analysis involves building timelines for different credible adversary paths to the target to determine whether there is high assurance that the corresponding adversary attack will be detected while there is enough time remaining for the response force to interrupt the adversary. The probability that the attack will be detected in time turns out to be the probability of interruption, P_I, for that attack.

Path analysis begins by modeling a series of concentric protection layers around a particular target under specific operating conditions against adversaries with specific capabilities as defined by the TA/DBT. The combination of these protection layers around a target defines a potentially large set of adversary paths.

Path analysis then determines one or more paths with the lowest PI among the set of adversary path; such a path is called the most-vulnerable or critical path. Most-vulnerable paths can be identifiedby inspection if the models of the protection layers are very simple or may identified using software tools that exhaustively examine all adversary paths through ASD's or networks representing the physical aspects of the facility.

Path analysis can also be used as part of a failure modes and effects study to determine how defeat of physical protection measures and subsystems may effect Probability of Interruption.
The principles of path analysis and its value will be demonstrated here using what are called Adversary Sequence Diagrams (ASDs) to represent the physical layers of protection around targets and all the potential paths.



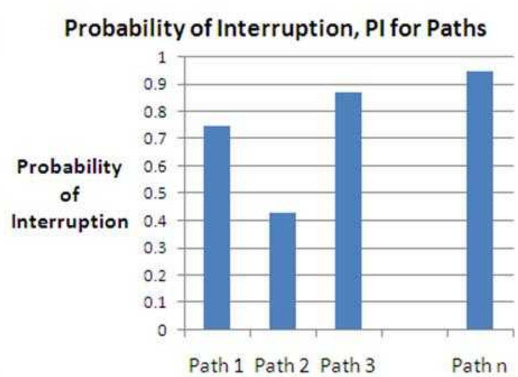


Figure XX. Adversary Sequence Diagram

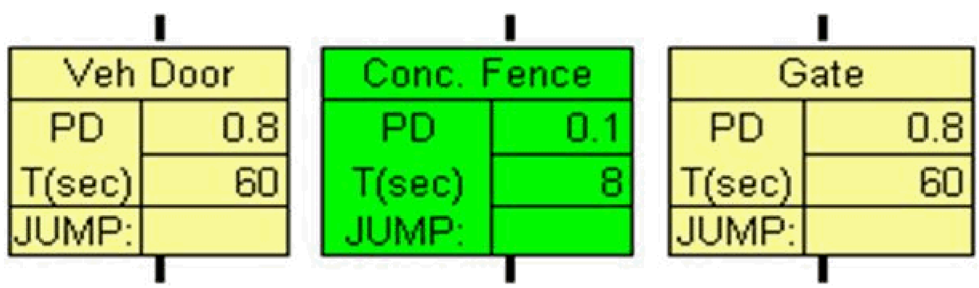
The left-hand side of Figure XX shows an ASD with 5 layers of protection. The second layer of protection (treating Offsite as the "0th" layer with no security) consists of a Personnel Portal, Vehicle Portal and Fence, which represent 3 ways to get through that protection layer. There are 4 paths shown on the diagram; one of them shown in green, starting with Offsite, then proceeding through a Vehicle Portal, then passing through the Wall and Roof, etc. The red, green, and blue paths may represent Paths 1, 2, and 3, respectively, on the right hand side. The vertical axis of the chart on the right-hand side measures the P_I for each path.

It can be seen that protection along the three paths shown is not balanced; Path 2 has a P_I about 60% of P_I for paths 1 and 3. We can also check to see whether this system meets regulatory requirements in terms of P_I:

- If the regulatory requirement is that P_I should exceed .4, then this system meets regulations but still has unbalanced protection;
- If the regulatory requirement is that P_I should exceed .6, say, then this system neither meets requirements nor is protection balanced.

In the second case we also know that P_E is not more than .6 based on P_I being greater than or equal to P_E.

By looking across a protection layer, one can see whether detection and delay are roughly balanced or not.



In the layer described above, both probability of detection (P_D) AND delay times are not balanced: the concrete fence has a much lower P_D and a much lower delay time, T.

Defence-in-depth can be assessed based on information about where Critical Detection Points (CDP's) fall along adversary paths. To demonstrate how to do this requires some more detail about path analysis.

An ***adversary path*** is an ordered series of actions against a target which, if completed, results in successful theft or sabotage. As an example an adversary may wishes to destroy a pump in a high security area. The path to do so might be: 1) penetrate a fence, 2) penetrate an outer door, 3) penetrate a wall, 4) penetrate an inner door, and 5) destroy the sabotage target (the pump).

P_I is defined as the probability that the response forces will arrive and deploy in time before the adversary has completed their attack. P_I is calculated using an adversary timeline and a response timeline. The figure below depicts the adversary timeline at the top, indicating the Task Time it takes the adversary to complete all of his tasks, and also the sensing opportunities along the timeline which may cause the adversary to be detected. Below the adversary timeline there is a comparison between the PPS Response Time (PRT) and the Adversary Task Time Remaining on the path after first sensing at each possible sensing opportunity.

If PRT < Adversary Task Time Remaining After First Sensing then the corresponding sensing opportunity is considered timely; if this is not the case, then the opportunity is not timely.[5] P_I is equivalent to the probability that the adversary is detected at least one of the timely sensing opportunities. For the example in Figure E-1, the first two sensing opportunities are timely, so P_I = P(Detection at Sensing Opportunity 1 OR Sensing Opportunity 2). The Critical Detection Point or CDP is the last sensing opportunity on the adversary timeline that is timely, in this case Sensing Opportunity 2.

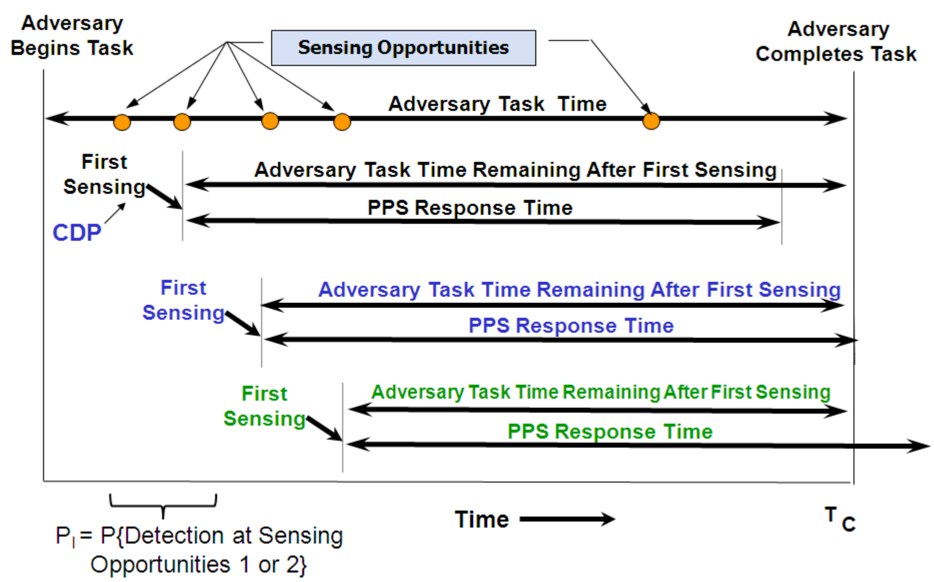


Figure E-1. Relationship between the Adversary Timeline and the Response Timeline

Within this context, detection defence-in-depth is then assessed by considering those detection measures that fall before or at the CDP on all paths. For example, detection and defence-in-depth is probably

[5] This model is called "timely detection" and not "timely sensing" because the timing for the beginning of the detection process is the sensing event; hence from a timeline perspective timely detection equates to timely sensing.

minimal if there is only one protection layer or line of sensors that is timely. Delay defence-in-depth can also be assessed by considering those delay measures that fall after the CDP on one or more paths.

The level of site detail and performance values used in path analysis will typically increase as requirements and design details are progressively developed; for example:

- Initial planning or early conceptual design: protection layers around protected areas, inner areas, and vital areas are assigned derived requirements, design details, and target performance values with these requirements, details, and values divided into those associated with authorized entry points versus protection along unauthorized routes. Where necessary, requirements, design details, and performance values will be assigned within these security areas.
- Conceptual – Detailed design: design details and performance values are assigned to path elements in an Adversary Sequence Diagrams (ASD's); see the figure below. Earlier in conceptual design the ASD may simply represent protection layers with a small set of elements, representing generic personnel and vehicle portals and barriers; as the design progresses the ASD will become more detailed. Note that the ASD shown depicts the PPS in terms of physical areas in the design, a higher level of detail than the protection layers around security layers. Information about adversary tactics and associated detection probabilities and delay times can be tracked for each of the elements within the ASD. Adversary action sequence diagrams for insider analysis fall within this set of representations.[6] PPS requirements will not only exist at protection layers but also within security areas based on needs for compartmentalization and surveillance, as examples.
- Detailed design: Design details and performance values are assigned with a spatial representation of the facility. This representation may range from an incremental improvement on an ASD (for example, keeping track of element-to-element delay times across protection layers) to a very-detailed representation of a site and facility(ties) using polygons ;

[6] Adversary action sequences typically include insider pathways for removal that are not important for outsiders, such as waste streams, ventilation ducts and drains, and administrative processes for sending equipment for maintenance.

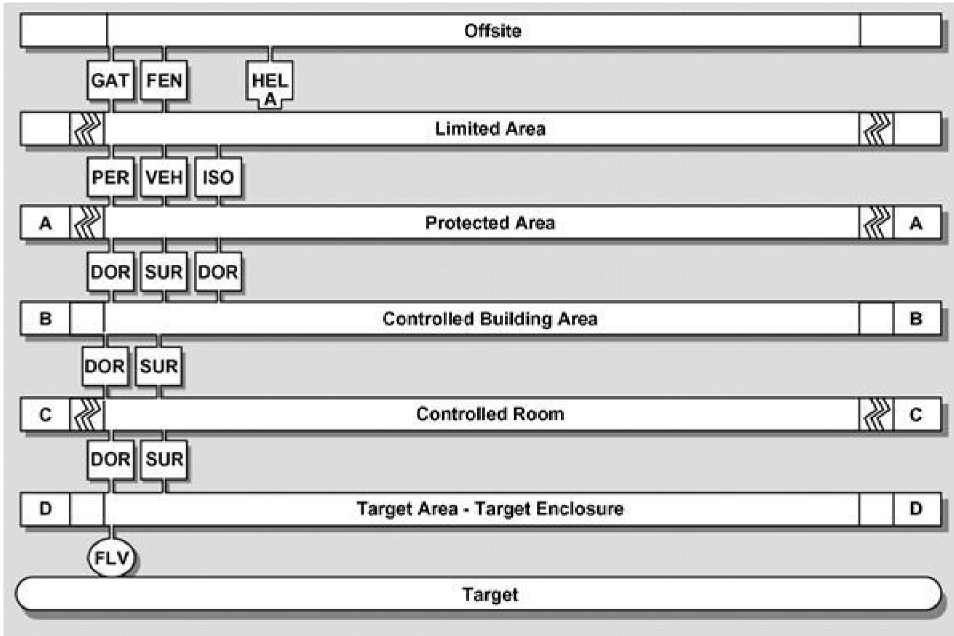


Figure Example of an Adversary Sequence Diagram

5.4.2 Scenario Analysis

The purpose of scenario analysis is to assess system effectiveness or the impact of changes to PPS capabilities or adversary capabilities on system effectiveness. Analyzing a scenario leads to a scenario outcome – either win or loss. But the focus of scenario analysis is on the capability drivers of outcomes; it is these that must be sustained, or improved, or – in the case of successful adversary capabilities – mitigated in order to ensure PPS system effectiveness. There are two approaches to scenario analysis: 1) analysis based on expert judgment and rules or heuristics; 2) analysis based on a free-flowing interaction of opposing forces, either through the structured discussion of a tabletop exercise, or in real-time simulation.

5.4.2.1 Scenario

A postulated or assumed set of conditions and/or events. Most commonly used in analysis or assessment to represent possible future conditions and/or events to be modelled, such as possible accidents at a nuclear facility. A scenario may represent the conditions at a single point in time or a single event, or a time history of conditions and/or events (including processes). Safety analysts use accident scenarios to describe and model plant response to potential accidents. An accident scenario, which usually has an initiating event superimposed on a proposed plant configuration, can be used to model system response, including various operator actions as appropriate. [4T]

- IAEA Nuclear Security Glossary, Draft v1.1, May 2014

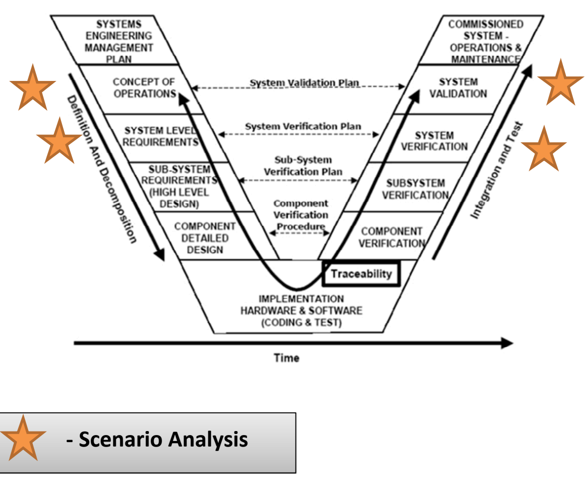
A scenario is a story of how events might unfold, given a postulated set of initial conditions and the interaction of opposing capabilities and actions. This story is developed through a structured process involving subject matter experts and real or postulated data. Inputs to scenario development include characterization of the protected assets and facilities, capabilities of the PPS and associated response forces, and a DBT.

5.4.2.2 Uses of Scenarios

How are scenarios to be used? Scenarios show how a static list of adversary capabilities might be employed in a hypothetical attack. Scenario analysis supports system-level PPS effectiveness analysis. As shown in the figure below, it also supports various systems engineering activities associated with PPS development including requirements definition, conceptual design, detail design, design verification, and system validation. Scenario analysis involves some degree of judgment & interpretation.

Analysis of a protected asset and associated PPS may reveal several broad adversary attack methods, as well as critical components that can severely degrade the PPS if attacked. It is probable that several scenarios may be required to adequately illustrate potential outcomes of attacks against all these elements. PPS components designed to incomplete scenarios may not completely fulfill system / mission level requirements. Scenarios must thus be both accurate and complete, to be useful.

Scenario Analysis in the PPS
Development Lifecycle



5.4.2.3 Elements & structure of a scenario

A scenario consists of four main elements:

- a characterization of the 1) protected asset, 2) protecting PPS, 3) postulated adversary, and 4) a threat plan and sequence of actions that would support adversary objectives

The data required to support the characterization activities is either collected through empirical testing or is estimated through various analysis techniques and methods. Those methods include performance data analysis, engineering analyses such as breaching / blast analysis, path analysis and insider analysis. Tabletop analysis and path analysis can support development of a plausible threat plan and sequence of actions. Path analysis by itself is insufficient to derive an adversary plan because its primary purpose is to identify imbalances in PPS detection and delay elements. Path analysis has very low resolution with respect to tactics and assumes that an adversary seeks to avoid detection for as long as possible. While this serves the purpose of identifying gaps in detection and delay, it is generally inadequate to the task of developing a plausible adversary plan.

1. Description of the protected asset. This starts with the asset itself.
    1.1. Can the adversary achieve a sabotage consequence with the protected asset, or must it be combined with other materials?   The analyst conducts rollup analysis to determine rollup risk. Is the condition of the asset constant, or does it change with respect to location, security, or other aspects during the course of facility operations? Could compromising the facility itself produce a sabotage consequence? The analyst may conduct fault tree analysis or vital area analysis to identify asset or facility components that could quickly lead to an unacceptable consequence if attacked.
2. Description of PPS & response force conops. Are there paths that circumvent effective response? The analyst may use path analysis to identify potential gaps in delay or timely detection, supplemented by terrain analysis to identify potential tactics or terrain that would support bypassing response elements. Are some PPS components vulnerable to compromise through covert or overt means? Here the analyst can apply technical analyses of facility structures and operational procedures to identify and quantify the vulnerability of PPS components to defeat through DBT defeat methods such as explosive breach, stealth and deceit tactics and others. Is the response force itself vulnerable to defeat due to inadequate survivability, mobility, firepower, communications, or procedures? The analyst seeks to determine vulnerabilities; i.e., weaknesses that can be exploited by an adversary.
3. Adversary characterization – with the DBT as a boundary condition, the security analyst develops an adversary capabilities list that describes the composition, capabilities, motivation & objective of a postulated adversary. These are formulated to support an objective of attacking one or more identified PPS or protected asset vulnerabilities to achieve the adversary objective.
4. Threat plan – finally, adversary capabilities and objectives are put together into a plan of action that describes the adversary attack paths, his sequence of actions and his tactical concept.

5.4.2.4 Scenario Sets

It may be necessary to develop several scenarios to address a variety of PPS vulnerabilities. Before developing individual scenarios, it may be necessary to determine the types of scenarios that will be required. The sample table below shows how adversary capabilities and PPS elements might be associated in the planning of a scenario set.

	Threat Objective		Attack Method		Tactics				Information	
Scenario Variables	Theft	Sabotage	Foot	Vehicle	Overt	Stealth	Deceit	Collusion	Passive Insider(s)	Active Insider(s)
Operating Conditions										
Operational Hours	1	5	1	5	1	5	1	9	1	5
Off Hours	2	6	2	6	2	6	2	10	2	6
Vault Open	3	7	3	7	3	7	3	11	3	7
Convoy	4	8	4	8	4	8	4	12	4	8
PPS Performance Elements										
Isolation Zone	1									
Fence	1									
Personnel Portal	2									
Vehicle Portal	2									
Door	3									
Wall	3									
Roof	4									
Vault	4									
Glove box	4									
Response Force	5									
Communications	5									
Network	5									
Power	5									

5.4.2.5 Scenario Development Best Practices

1. Use of Experts – experts in mission planning, tactics, techniques, protected asset operations & conditions should be used to ensure an accurate and plausible scenario.
2. Technical analyses such as path analysis, and performance data should be incorporated where possible.
3. Scenarios should be independently reviewed by experts and approved by stakeholders and risk owners.
4. Scenarios should be representative of the bulk of the problem space, not just outliers.
5. Scenarios will be used for a variety of system engineering activities, including system effectiveness analysis. It will be important to maintain configuration management of approved scenarios.

Appendix to Section 5 – Systems Engineering

Evaluation of PPS Effectiveness of a Nuclear Facility – Systems Engineering Principles

Introduction

"Effective" is defined as "producing a decided, decisive, or desired effect." Therefore, to determine a system's overall effectiveness, one must first define in measurable and verifiable terms the system's desired qualities and functions. This is done pre-design via systems engineering and requirements definition processes, followed by a series of in-design, post-design, in-construction, and post-construction test verification processes. In complex systems, quantifying effectiveness may be the result of combining sub-system measurements, each represented by simulation results, mathematical or statistical calculations, or experimental test data measured against the requirements baselines. When defining requirements, one may assign "TADI" definitions which state how each requirement is to be verified: by test, analysis, demonstration, or inspection (TADI). There are openly-available standard processes noted below that define these concepts.

Overview

Nuclear security is not an end in itself, but an enterprise of activities that support the safe use of nuclear materials for various purposes. Nuclear security must therefore be understood both in terms of its constituent activities and the external context in which it exists. Effective nuclear security is based on an integrated set of security systems, best practices, policies, plans, procedures and organizations. Security organizations must be effectively structured, trained and managed. Security systems, the focus of this [handbook], must be effectively designed, implemented, operated and maintained to function effectively. The [DEPO] process outlined [reference] provides a framework for understanding the special considerations associated with designing and developing a physical protection system. Applying this framework to the task of developing a PPS involves the effective integration of several bodies of knowledge by many stakeholders. PPS design teams, site operators, and security program managers are all involved in the development and must interact within standard frameworks to avoid confusion and rework. It is important that security professionals be cognizant of the fundamentals of these disciplines so that they can ensure effective implementation of a PPS. Following is a partial list of essential disciplines that inform the [DEPO] process[7].

Examples of Standards

- Systems Engineering, EIA-632, Engineering of a System. Systems engineering (SE) ensures that the functions, internal / external interfaces, architecture and operation of a PPS all function to meet system requirements and the overall objective and purpose of the system. SE integrates requirements engineering with system architecture development and design definition to ensure that the PPS meets requirements and is effectively designed. PPS systems effectiveness analysis is an instance of systems analysis, which is a normal systems engineering activity.

---

[7] See http://sebokwiki.org/wiki/Relevant_Standards for a comprehensive taxonomy of systems engineering activities & associated international standards.

- Risk management, ISO 31000:2009, Risk Management - Principles and Guidelines. The purpose of the PPS is to reduce nuclear security risk. Many of the PPS analysis activities, such as scenario analysis, come from Risk Management Frameworks (RMF).
- Requirements, ISO/IEC/IEEE 29148 Systems and software engineering – Requirements Engineering. Effective requirements engineering ensures that enterprise policies, user needs, and other mandatory considerations are formulated in a way that supports effective PPS design development and verification of PPS system effectiveness.
- Architecture, ISO/IEC/IEEE 42010 Systems and software engineering – Architecture Description. Systems architecture defines the physical and functional system in a way that ensures that the PPS implements all requirements efficiently and effectively.
- Project management, **ISO 21500:2012**, *Guidance on Project Management. Poor project management, with resulting cost overruns or schedule slips can be a source of nuclear security program risk, since security projects often compete with resources required to operate the protected power plant. PPS developers should be conversant with the basic principles of project management as part of the development process.*

- *Continuous Quality Improvement,* ISO 9001:2015, *Quality Management System*. [http://www.iso.org/iso/iso_9000] ISO 9001:2015 establishes criteria for a quality management system. It is the only standard in the 9000-series family to which one can create certifications (although not required). It can be used by any organization, large or small, regardless of activity. Over one million companies and organizations in over 170 countries are certified to ISO 9001. This standard is based on a number of quality management principles including a strong customer focus, the motivation and implication of top management, the process approach and continual improvement. The seven principles, including a process approach (#4) and evidence-based decision making (#6) are explained in more detail at the ISO website. Using ISO 9001:2015 helps ensure consistent, good quality results.
- *Construction Specifications Institute, CSI Master Format Outline:2014 [* http://csinet.org/numbersandtitles *]. Complex construction projects require integration of many complicated sub-system technologies. Industry has developed a set of standard guidelines for organizing construction design specifications. These serve not only to unify the process across industry, but also organize and streamline the design-through-construction implementation. The master format outline, while not necessarily comprehensive, can serve as an integration checklist to assist with blending security and communications (C4I) designs seamlessly into other typical construction projects. Electrical, Communications, and Electronic Security topics are addressed in sections 26-28 respectively. Other sections may also contain security-related items, such as Openings (doors & windows, sec. 8), Equipment (e.g. parking gates, Sec. 11), and Exterior (e.g. fences & gates, sec. 32 sub. 31).*

Systems Engineering Methodology Overview - Concepts & Figures

The fundamental processes for engineering a system are shown in the five boxes of Figure Appendix 5-1 below. This section of the implementation guide focuses upon "evaluation of PPS effectiveness" which resides in the "technical evaluation" box. As this box is interconnected to all of the other boxes, it should be noted that technical evaluation may be applied to any part of the overall system or any subsystem or component, at any time, as needed to ensure that a successful "system product" exits the right side of the diagram.

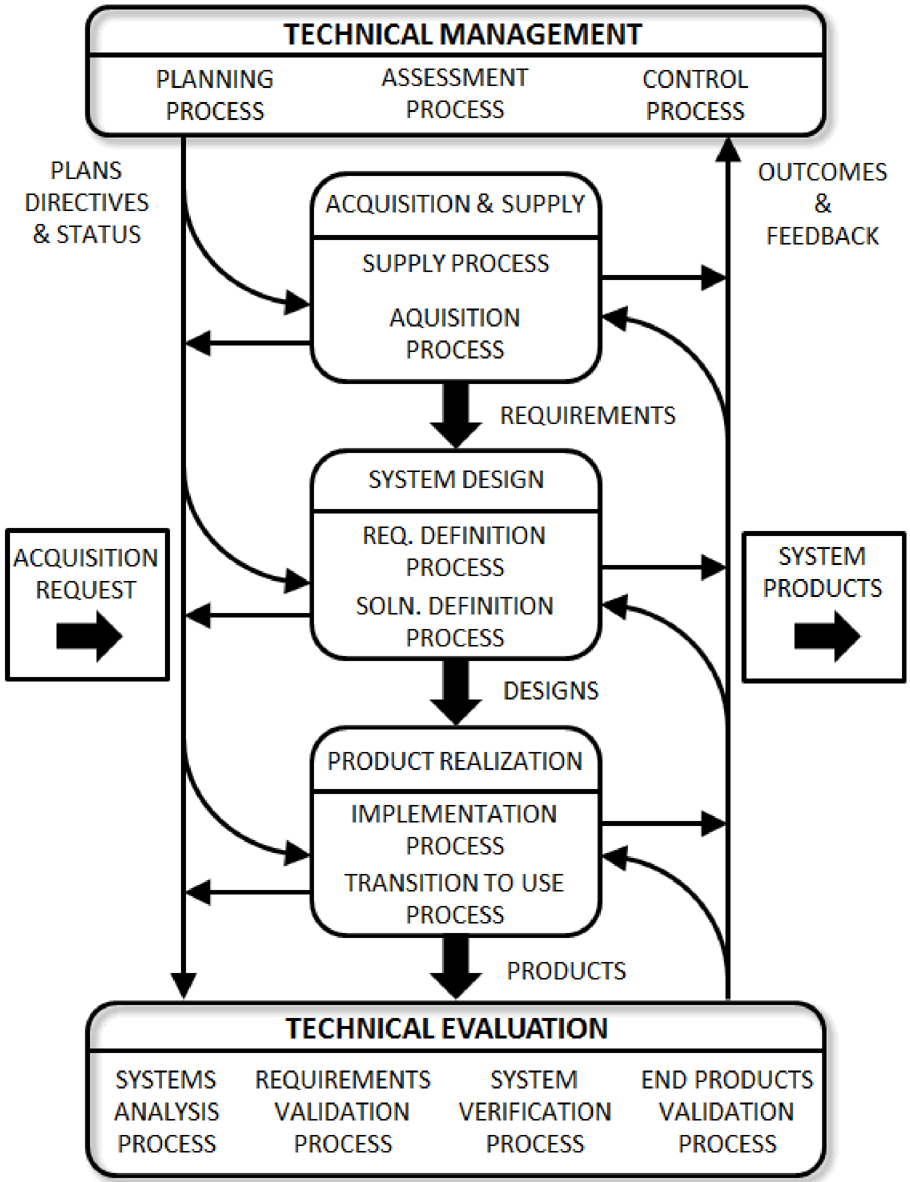


Figure Appendix 5-1 - Ref: EIA-632 Processes for Engineering a System

Figure Appendix 5-2 is an example of the Systems Engineering "V." It shows the overall process of development, assurance and testing, and construction of a project from concept through retirement or replacement/upgrade.

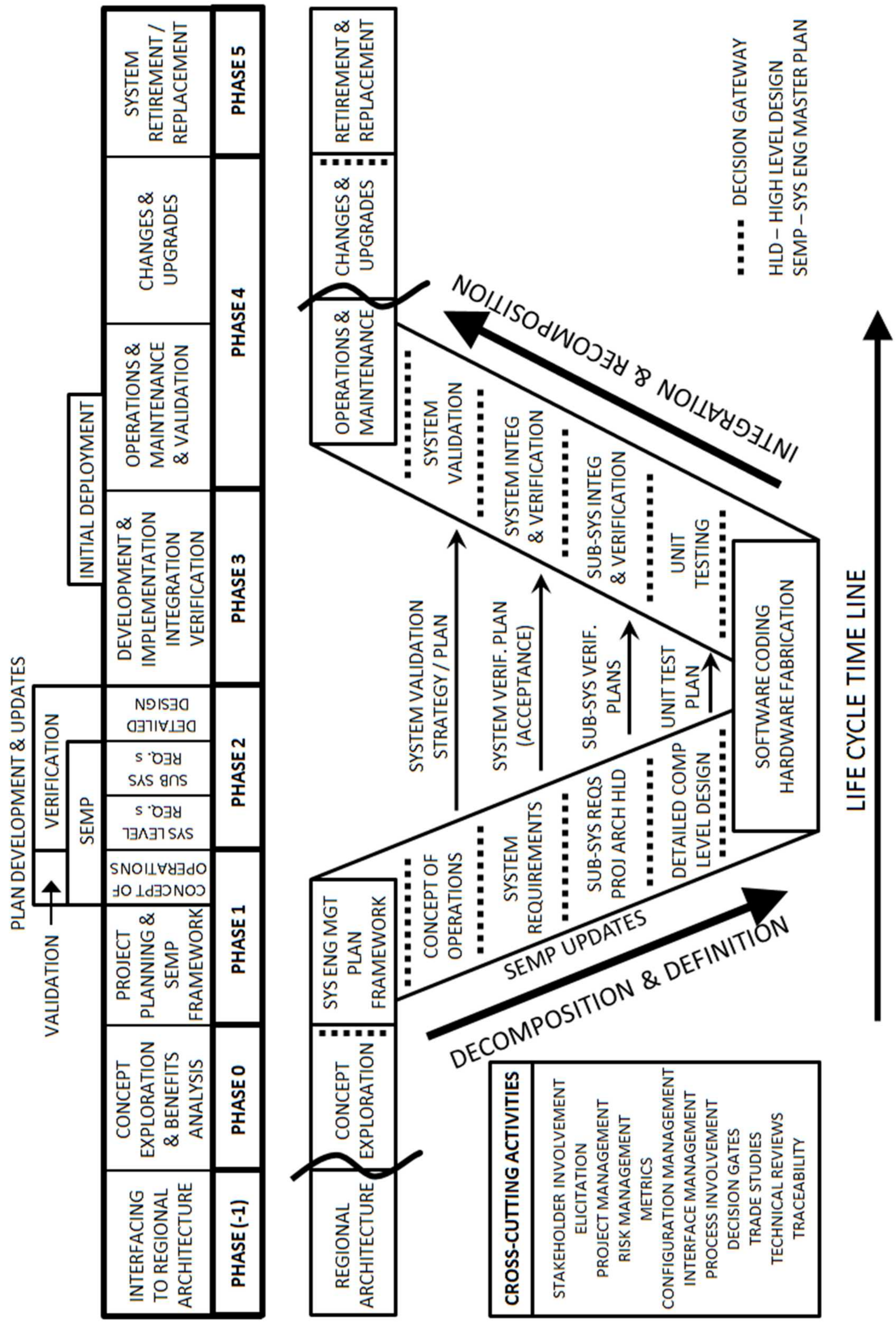


Figure Appendix 5-2 - Ref: EIA-632 Systems Engineering “V” – Project Lifecycle and Task Flow

Evaluating PPS effectiveness begins in the early "concept exploration" phase. Ideally, PPS design will be integrated seamlessly into the features of the project or site the PPS is intended to serve. Evaluations at this early stage may include modeling and simulations of adversary threat activities, intrusion path analyses, and table-top exercises to determine what form of PPS might be viable. Initial rough concepts may be rapidly formulated from existing toolsets and knowledgeable experts who can draw upon past successful experiences. Additionally, such evaluations may yield information or configurations which could provide optimal design and performance advantages, with those results supporting all subsequent Phase 1 & Phase 2 activities in the left leg of the systems engineering "V." An early market analysis is often included to determine what new products and technologies may yield optimal initial PPS performance or extended life cycle advantages. Finally, some early statistical mathematics and theoretical probability of effectiveness (Pe) calculations may be used to validate the viability of the conceptual PPS. Such early activities can prevent wasteful funds expenditures in failed design and construction, schedule-breaking rework, or implementation of a later-discovered ineffective PSS.

Evaluation analyses continue throughout the early, middle, and final design phases. These may include a repeat of the conceptual exercises using the progressively-more-defined engineering details to support or prudently reset designs as they evolve. New component and subsystem performance tests, along with iterative integration tests, are applied as the design grows and forms into the final fully-functional system. These functions are illustrated in Phase 3 along the right-leg of the systems "V." Back checks are performed along the arrows within the "V" to ensure that the progressing designs and constructions continue to meet the originally intended and documented parameters. Changes can be made to the original parameters if necessary, but such core modifications must be made with care so as to preserve the original PPS intent and functions, and must be vetted and accepted by the customer and approval authorities prior to change. Confirmation of retained PPS functions by the knowledgeable original designers is recommended, as such changes may be sought by other entities (e.g. construction contractors) that may prioritize monetary or schedule gains over an effective PPS.

Knowledgeable inspectors are key performers throughout the construction phase of the PPS. These inspectors ensure each installation portion is correctly executed prior to overlaying additional construction. For example, it can be very costly to remove and rebuild a road that has covered an inappropriately constructed concrete duct bank with inadequate embedded communications conduits. Key inspections should be made and documented prior to any critical, expensive or permanent progressions to the construction project. It is often recommended that the designers conduct pre-construction meetings with the inspectors and constructors to discuss critical features of the PPS design and ensure understanding of the design intent. Such educational meetings may be conducted at the beginning of and throughout construction and are invaluable to the success of the project.

Phase 4 (operations, maintenance, upgrades) and Phase 5 (retirement, replacement) provide additional opportunities for systems effectiveness analyses. Operations (CONOPS) effectiveness may be improved using mod-sim exercises leveraging security response force feedback about the installed system in its unique environment – including corrections of some operational details that may have been missed in the original designs. Maintenance and upgrades must be carefully controlled to prevent degradation of PPS performance via substandard care or use of inappropriate replacement components. Finally, analysis may be applied to safely deconstruct a PPS at strategic times during facility dismantlement, or to create a segmented approach to replacing or upgrading an aging PPS system while keeping the current system active.